ZoomAir Wireless Bridge™

Installation Guide
&
Reference Manual

NOTICE

This document contains proprietary information protected by copyright, and this Manual and all the accompanying hardware, software, and documentation are copyrighted. All rights are reserved. No part of this document may be photocopied or reproduced by mechanical, electronic, or other means in any form.

The manufacturer does not warrant that the hardware will work properly in all environments and applications, and makes no warranty or representation, either expressed or implied, with respect to the quality, performance, merchantability, or fitness for a particular purpose of the software or documentation. The manufacturer reserves the right to make changes to the hardware, software, and documentation without obligation to notify any person or organization of the revision or change.

All brand and product names are the trademarks of their respective owners.

© Copyright 2001
All rights reserved.

Contents

INTRODUCTION 5

OVERVIEW.. 5
CONTENTS OF THE ZOOMAIR WIRELESS BRIDGE PACKAGE 6
CONSIDERATIONS BEFORE SETTING UP 6
OPTIONS FOR MANAGING THE ZOOMAIR WIRELESS BRIDGE 7
WIRELESS BRIDGE SECURITY 8

CHAPTER 1 CREATING A WIRELESS BRIDGE................. 9

SETTING UP... 9
General Strategy 9
Setup Procedure 12
TESTING AND TROUBLESHOOTING 16

CHAPTER 2 WEBMANAGE ACCESS............................... 19

ACTIVATING WEBMANAGE 19
System Requirements for Activating WebManage 19
SYSTEM INFORMATION.. 20
Admin security 20
Device Information... 21
Time... 21
NTP... 22
Save Changes... 22

CHAPTER 3 WIRELESS BRIDGE CONFIGURATIONS...... 23

THE ZOOMAIR WIRELESS BRIDGE DEFAULT SETTINGS 23
SSID AND CHANNEL SETTINGS.. 25
WIRED EQUIVALENT PRIVACY (WEP).. 27
ADVANCED SETTINGS 29
DEVICE IP ADDRESS 31
MONITORING THE ZOOMAIR WIRELESS BRIDGE 32
QuickView Monitor.. 33
Diagnostics Monitor 34
Statistics Monitor 35
USING THE ZOOMAIR WIRELESS BRIDGE REPORTS 36
MAINTAINING THE ZOOMAIR WIRELESS BRIDGE........................... 38
Accessing Maintenance in WebManage.. 39
Backup System Code 39

Upgrading the System Software..40
Restarting the ZoomAir Wireless Bridge..41

APPENDIX A ASSIGNING NEW IP ADDRESSES TO ZOOMAIR WIRELESS BRIDGE UNITS.............................43

PING TESTING THE ZOOMAIR WIRELESS BRIDGE-PC CONNECTION ... **47**

APPENDIX B LED INDICATORS 49

LAN LED INDICATORS.. **49**
WIRELESS LED INDICATORS.. **50**

APPENDIX C CONSOLE COMMANDS..............................51

SETTING UP THE CONSOLE **51**
CONFIGURING OTHER PARAMETERS **52**
Get Commands: Displaying the Configuration....................................52
Set Commands: Changing the Configuration......................................54

APPENDIX D THREE-WAY WIRELESS BRIDGE SETUP...57

APPENDIX E REGULATORY INFORMATION...................59

Introduction

Your ZoomAir Wireless Bridge™ provides ease and flexibility in linking two wired Local Area Networks (LANs). This Introduction includes the following:

- *An overview of the ZoomAir Wireless Bridge and its feature set*
- *A list of the components included with the ZoomAir Wireless Bridge unit and other items you need*
- *A summary of the ZoomAir Wireless Bridge management options and security features.*

Overview

Two ZoomAir Wireless Bridge units form a wireless bridge that links two wired LAN segments (also referred to as "networks" or "wired networks" in this manual). The Bridge units are IEEE 802.11b DSSS-compliant (Direct Sequence Spread Spectrum technology). They may be set up in two different buildings or in two sections of the same building. Each Bridge unit is connected to a wired network, and the two units transfer information between the networks over a wireless link.

Note: For a description of a three-way wireless bridge setup, refer to Appendix D, on **page 55**.

Using the Bridge, you can instantly connect workgroups located in different buildings, without having to worry about wiring them together or paying the recurring costs of a wired link (for example, a T1 line leased from a telco provider), burying a cable between buildings, or adding wiring in a building. The ZoomAir Wireless Bridge is particularly well suited to campus environments, where line-of-sight installation is straightforward. The range of the wireless link is up to 1 kilometer (3,000 feet), so that support of a local branch office in a neighborhood area is also possible, with the same benefits. Again, a line-of-sight path between the two endpoints provides the best results.

When connected by the wireless Bridge, users on LAN segments on either side of the Bridge have complete access to devices connected on both sides of the Bridge, including servers, databases, and printers. See the illustration of the wireless Bridge setup on **page 10**.

Contents of the ZoomAir Wireless Bridge Package

In addition to this manual, your ZoomAir Wireless Bridge package includes the following components:

- Two ZoomAir Wireless Bridge base units
- Two ZoomAir Cards (11 Mbps)
- Two Ethernet 10BaseT straight-through cables to connect the ZoomAir Wireless Bridge LAN ports to a network hub
- Two RJ-45 cables with RJ-45 to DB-9 adapters for connecting a Bridge console port to the serial COM port of a computer
- Two 12-VDC power adapters
- Two directional antenna sets, containing the following:
    - Two 13 dBi directional antennas
    - Two 3-meter coaxial cables to connect the directional antenna to the ZoomAir Card
    - Two antenna mounting brackets
- One roll of coax seal (60 inches).

Considerations before Setting Up

Your plan for the permanent location of the ZoomAir Wireless Bridge should include the following:

Power: You will need an electrical outlet for the power adapter.

Ethernet: The ZoomAir Wireless Bridge must be located near an available Ethernet connection.

Antenna: The ZoomAir Wireless Bridge should be placed close to an optimal antenna location. For ideal building-to-building transmission, each Bridge unit would be near an antenna that is outside a window, and you would be able to see one antenna from the other antenna, possibly with the aid of binoculars. Large obstructions between the two antennas may impair communication.

Options for Managing the ZoomAir Wireless Bridge

You can configure and maintain your ZoomAir Wireless Bridge in one of three ways:

- A console port lets you configure a ZoomAir Wireless Bridge unit directly from any computer by entering commands through a terminal emulator, such as HyperTerminal, and sending them through a serial port.

Note: We recommend that you use a console port to begin the installation procedure by changing the default IP addresses of your ZoomAir Wireless Bridge units.

  To configure and maintain the ZoomAir Wireless Bridge through the console, we recommend that you use the supplied RS-232 cable and RJ-45 to DB-9 adapter. You may also need a second adapter to match the DB-9 adapter to your computer's serial port: a DB-9 to DB-25 adapter for a PC or a DB-9 to 8-pin Mini-DIN for a Macintosh. See your computer documentation for more details.

  For console command instructions, turn to Appendix C, **page 49**.

- The WebManage™ utility allows you to use a compatible Web browser running on any computer on the network to configure the ZoomAir Wireless Bridge. WebManage is password-protected so that only authorized administrators can set or modify the ZoomAir Wireless Bridge settings. For additional information on WebManage, refer to Chapter 2, **page 17**.
- A Telnet application allows you to log onto the console functionality remotely by telnetting to a ZoomAir Wireless Bridge unit and executing console commands as though connected through the console port. To log on via Telnet, use the IP address that you assign to the Bridge unit, and log on with your username and password.

Wireless Bridge Security

You can add security features to your wired network. See Chapter 3 for more information. Wireless LANs that conform to the 802.11b or 802.11-DSSS standard provide three security measures:

- A unique network name called the Service Set Identifier (SSID).
- A channel number, which is similar in concept to the channels used in cordless telephones.
- Wired Equivalent Privacy (WEP), which provides a way of creating an encrypted "key" and locking out anyone who does not have the key.

The ZoomAir Cards included with the ZoomAir Wireless Bridge units are IEEE 802.11b-compatible, using DSSS technology. This provides 11 Mbps symmetrical data rates using spread spectrum technology. Spread spectrum signals are inherently difficult for unauthorized users to decode.

Also, both of your Bridge units must use a special SSID to be recognized as part of the bridge link. An SSID is configured to guarantee that only the device with that SSID can be part of the link. Bridge units boxed in pairs are shipped with identical SSIDs.

Finally, the Bridge's WEP software provides security that often equals or exceeds that of a wired bridge.

1

Creating a Wireless Bridge

In Chapter 1, we explain how to do the following:

- *Select a location for your ZoomAir Wireless Bridge units*
- *Set up your ZoomAir Wireless Bridge units.*

Setting Up

To create a wireless bridge, you need a pair of ZoomAir Wireless Bridge units and antennas (included in the Bridge package), one of each at the two ends of the bridge. If you wish to manage the units remotely via WebManage or Telnet, ask your system administrator for two IP addresses, one for each Bridge unit.

If you have a DHCP server, these two IP addresses must be outside of the range of your DHCP pool.

Note: LAN segments on both sides of the bridge must be on the same subnet. All PCs and devices on these segments must share the same TCP/IP subnet address.

In this chapter, we describe the following:

- Where to install the ZoomAir Wireless Bridge units
- How to connect the Bridge units to your LANs
- How to orient the antennas.

General Strategy

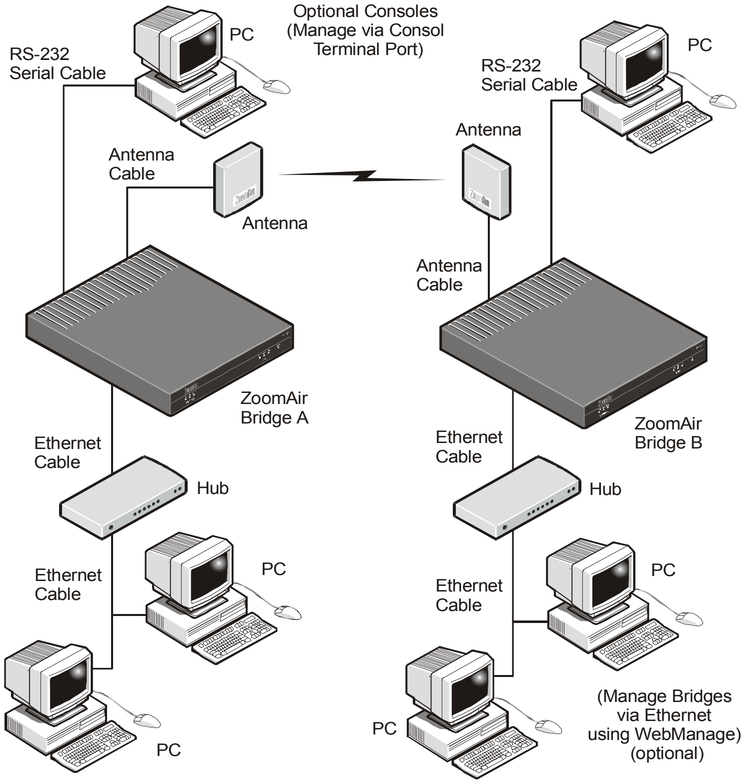
The two ZoomAir Wireless Bridge units must have the same SSID, and they must be set to the same channel. The default factory settings satisfy these requirements.

You will have a working wireless bridge when you do the following:

1. Find a suitable location for your Bridge units.
2. Assign a new IP address to each of the Bridge units through a console port (optional).
3. Physically connect each unit to a wired network.
4. Install and orient an antenna on each unit.
5. Establish a wireless link between the Bridge units.
6. Test the wireless link.

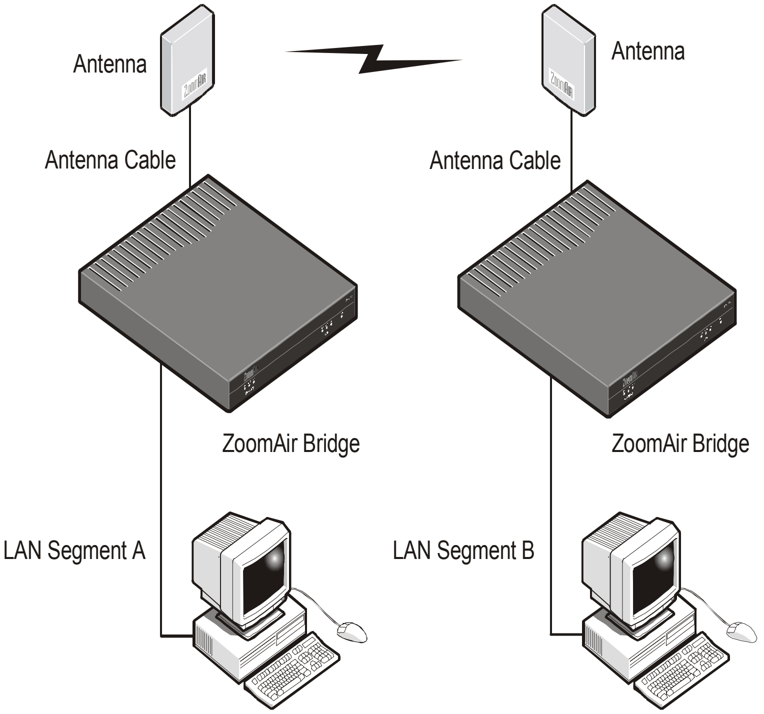
Wireless Bridge setup with a hub

The following graphic illustrates how two ZoomAir Wireless Bridge units form a wireless bridge between two wired networks when a hub is used:



Wireless Bridge setup without a hub

The following graphic shows an alternate wireless bridge setup, in which a PC is connected directly to a ZoomAir Wireless Bridge unit without a hub:



If you are connecting the Ethernet port of a PC directly to a ZoomAir Wireless Bridge unit, without a hub, you must use a crossover Ethernet cable between the LAN port of the Bridge unit and the Ethernet port of the PC. This cable is not included in your Bridge package.

Setup Procedure

Finding a suitable location for the ZoomAir Wireless Bridge

Each of your ZoomAir Wireless Bridge units must be located so that it can pick up radio signals from its peer unit. The range of the ZoomAir Wireless Bridge is approximately 2.5 miles at 2 Mbps.

Radio wave obstruction: The Bridge range depends on the attenuation characteristics of objects that may lie in the path of the wireless link. For indoor installations, this may include walls and floors. Outdoors, signal loss depends on the terrain and the density of foliage that may be in the path of the radio waves.

In addition, glass reflects the radio waves used by the ZoomAir Wireless Bridge. Therefore, outdoor mounting of the antenna is advised when the Bridge spans two buildings. There may be some attenuation through heavy snowfall.

Note: There is no significant attenuation through fog or rain at a range of 1km for the 2.4 GHz carrier used by the ZoomAir Wireless Bridge.

Assigning new IP addresses to your ZoomAir Wireless Bridge units

The two ZoomAir Wireless Bridge units in your package initially have the same factory default IP address. To manage the Bridge units through WebManage or Telnet, however, each must have a unique IP address, provided by your systems network administrator. We recommend that you assign IP addresses and manage the Bridge units through WebManage, but for the initial assignment of IP addresses, you should use a console. Thereafter, you can use a console, Telnet, or WebManage to assign these addresses.

We also recommend that you arrange a trial setup of your Bridge units to verify proper configuration. You can place the two units at opposite ends of a room, for example, to reduce the chance of other variables interfering with your test. Thus, you can verify the Bridge configuration without worrying about the integrity of your radio link.

To manage your ZoomAir Wireless Bridge units through WebManage or Telnet, assign IP addresses to the units. Refer to Appendix A, **page 41**, for instructions.

Connecting your ZoomAir Wireless Bridge to a wired network

To create a wireless bridge, follow these steps:

1. With power off, insert a ZoomAir Card into each of the two

ZoomAir Wireless Bridge units.

Note: The ZoomAir Cards cannot be hot-swapped. You must power down your ZoomAir Wireless Bridge each time you insert or remove a ZoomAir Card.

⚠ Do not force in the ZoomAir Card because the pins may break. The ZoomAir label and the antenna connector should be facing up.

2 Plug one end of the included Ethernet 10BaseT straight-through cable into the LAN jack on the ZoomAir Wireless Bridge unit. Plug the other end of the cable into a hub.

Note: Do not use the uplink connector on the hub. The ZoomAir Wireless Bridge is configured like a NIC card (DTE).

3 Plug the power adapter into the 12-VDC jack on the ZoomAir Wireless Bridge. Then plug the power cable into an AC outlet.

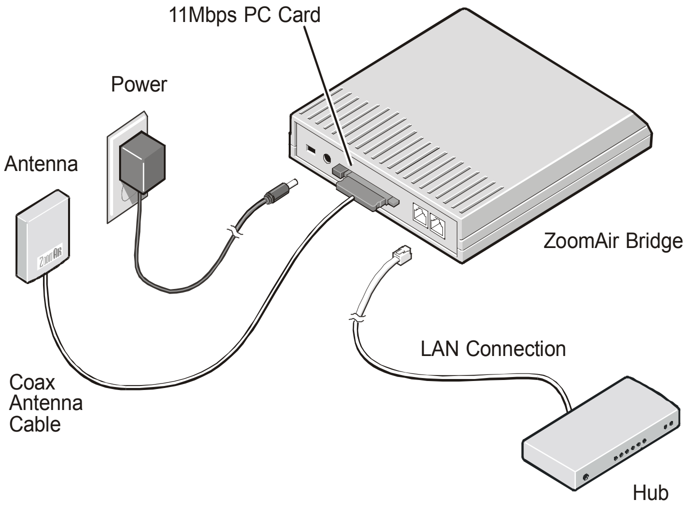
⚠ **CAUTION** Use only the power adapter that is supplied with the ZoomAir Wireless Bridge. Adapters may look similar but have different voltages.

4 Connect the antenna and fine-tune its orientation. Refer to **page 14** for details.

5 Turn on the power switch at the back of the unit. Orient the ZoomAir Wireless Bridge so that the LEDs are visible. Check the **ON** LED to make sure that the unit is receiving power. If it is, the light is green. It usually takes less than one minute for the ZoomAir Wireless Bridge to boot up.

6 Repeat this procedure to connect your peer Bridge unit to its wired LAN network.

The following graphic illustrates the setup of the components you need to create one side of a wireless bridge.



Installing and orienting the antenna

When each of the Bridge units is connected to a network, a wireless link must be established between the Bridge units. This requires aiming and adjusting the antennas and testing for an optimal connection. At the conclusion of this step, your wireless bridge will be operational. Do the following:

1 Mount the two antennas from your Bridge package so that the face of each aims toward the other. Make sure to minimize the number and size of any barriers in the line of sight between the antennas. (See **page 12** for a partial list of materials that are opaque to the radio signals of the ZoomAir Wireless Bridge.)

> **Note:** The antenna aim may be off by as much as 15 degrees in either direction from side to side, or about 10 degrees in elevation, without materially affecting the link.

2. Insert a ZoomAir Card into each Bridge unit, if you haven't done so already.
3. Connect each antenna to a ZoomAir Card with the included coaxial cable.

Note: The cable ends are not weatherproof. It is therefore important not to expose these sections of the cable to rain or to moisture from any other source.

For more information on antennas, refer to the Antenna Options and Installation Instructions flyer in your ZoomAir Wireless Bridge package.

Applying the coax sealant

Provided in your Bridge package is a roll of coax sealant that you can use to protect the outdoor cable couplings from moisture. Follow the directions on the seal package to apply the sealant in the following locations:

- Any exterior cable coupling
- Any through-the-wall run.

Testing and Troubleshooting

Note: Your Bridge unit may require resetting after a severe electrostatic discharge event.

After your wireless bridge is set up, you can run some simple tests to be sure everything is working. You should test the wireless connection by following the section Using the ZoomAir Wireless Bridge Reports on **page 34**. The reports allow you to view the state of the peer Bridge unit via WebManage.

After you have verified the link between the peers, if using Microsoft PCs, a fast, reliable way to check if a particular client is reachable is to go to **Start | Find Computer**, and enter the name of that client. The client should be on the opposite side of the bridge from where you conduct the connection test. If you can see the client, the bridge is operational.

Try exchanging files between PCs across the bridge from each other. Try to print from a computer on one side of the bridge to a printer on the other side of the bridge. If you have difficulty doing so, or if you choose not to use the Web browser to assign IP addresses, try the ping test, described at the end of Appendix A, **page 45**.

2

WebManage Access

After you have set up unique IP addresses for your ZoomAir Wireless Bridge units through the console, as described in Appendix A, you can use the WebManage utility to configure and monitor your ZoomAir Wireless Bridge units.

Note: If you want to continue using the console after making the initial setup changes, refer to Appendix C, on **page 49**.

Activating WebManage

To activate the WebManage utility, start your Web browser and type in the IP address you assigned to the ZoomAir Wireless Bridge; e.g., **http://192.168.0.240**.

Note on Proxy Servers and WebManage: If you have a proxy server on your LAN, make sure that the proxy settings for your browser are appropriate for the LAN. Consult the manual or online help for your browser if you have difficulty accessing WebManage.

System Requirements for Activating WebManage

The client must have Netscape Navigator (NS) or Internet Explorer (IE) 4.0 or later installed. The system must be configured to connect via a LAN. Also:

- Both Java script and Java must be enabled
- At least 640 x 480 resolution is recommended
- A 14" monitor or larger is recommended

Browser-specific settings

For Internet Explorer 4.0 to display WebManage correctly, you must change the IE default configuration. If using IE:

1. Click **Tools | Internet Options | General Page | Temporary Internet Files | Settings.**
2. Click the radio button next to **Every visit to the page**, and then click **OK** twice.

> **Note:** The IE configuration procedure varies among versions of IE.

If using Netscape Navigator:

1. Click **Edit | Preferences | Advanced | Cache**.
2. Under **Document in cache is compared to document on network**, choose **Every Time**.

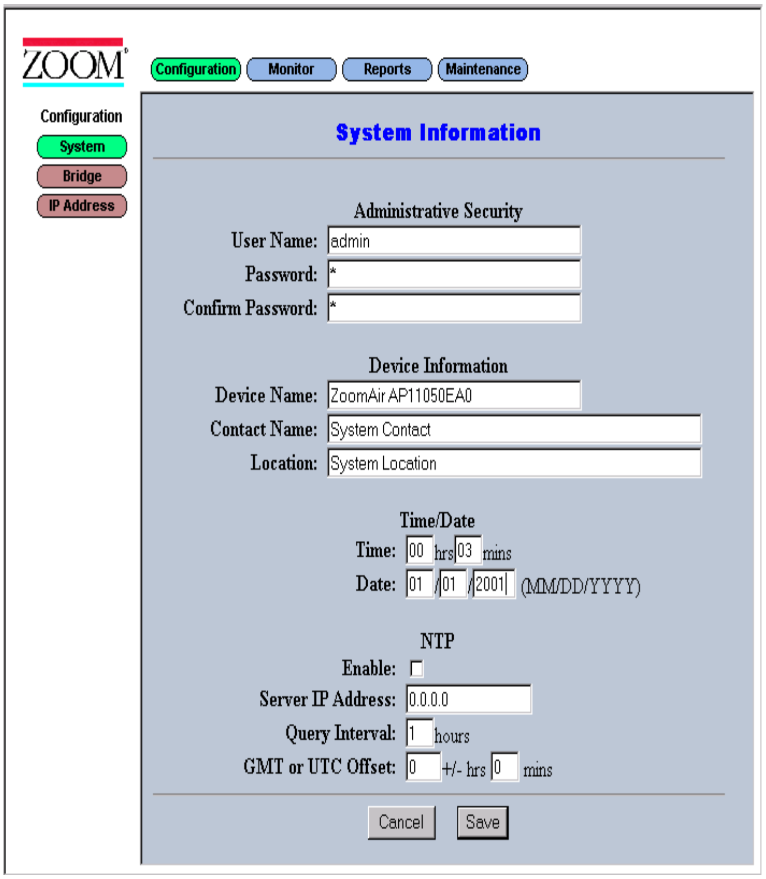
See your browser instructions if you need help.

System Information

Admin security

The first time you access WebManage, you will see the **System Information** page with text boxes for you to enter your user name, password, and other information.

After that, when you access WebManage, you will be prompted for your user name and password. See the following screen shot:



System Information

Administrative Security

User Name: admin
Password: *
Confirm Password: *

Device Information

Device Name: ZoomAir AP11050EA0
Contact Name: System Contact
Location: System Location

Time/Date

Time: 00 hrs 03 mins
Date: 01 / 01 / 2001 (MM/DD/YYYY)

NTP

Enable: ☐
Server IP Address: 0.0.0.0
Query Interval: 1 hours
GMT or UTC Offset: 0 +/- hrs 0 mins

Device Information

Type in the following in the text boxes:

Device Name: Enter the name for this unit.

Contact Name: Enter the administrator name.

Location: Enter the location of this unit.

Time

Set the current time and date if there is no NTP Time Server available on the network. When the time and date are set, whether manually or through an NTP server, the ZoomAir Wireless Bridge can stamp each log and diagnostic message with a time and date.

Note: The time should be set last because it will reset to the default when the unit is restarted.

NTP

The ZoomAir Wireless Bridge has the ability to obtain the date and time from an NTP server; it does not have an internal time-of-day clock. You can configure the ZoomAir Wireless Bridge with the IP address of an NTP server on your network and indicate how often the NTP server should check the current time.

Save Changes

Click **Save** to save the configurations, or click **Cancel** to edit the configurations.

3

Wireless Bridge Configurations

This chapter covers the topic of wireless bridge configurations in the following sections:

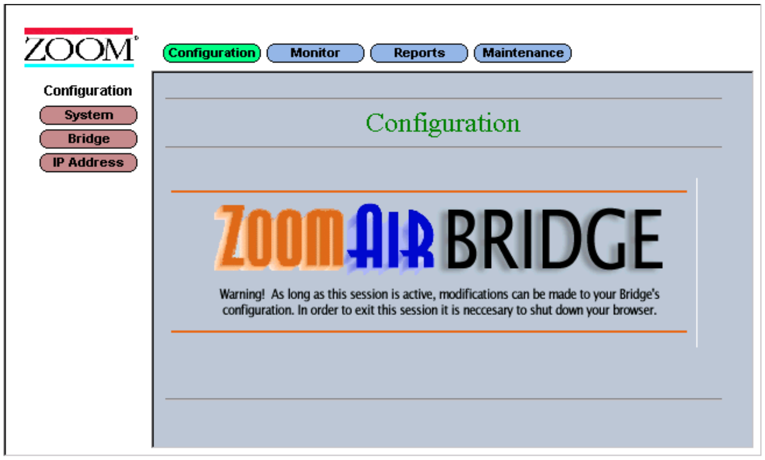
- *Verifying the ZoomAir Wireless Bridge default settings*
- *Configuring SSID settings and channel settings*
- *Configuring Wired Equivalent Privacy (WEP) settings*
- *Configuring the IP address of the ZoomAir Wireless Bridge*
- *Monitoring the ZoomAir Wireless Bridge*
- *Using the ZoomAir Wireless Bridge reports*
- *Maintaining the ZoomAir Wireless Bridge.*

The ZoomAir Wireless Bridge Default Settings

Proceed to the subsequent sections in this chapter for instructions on how to configure your wireless bridge. Return to this section if you need to verify the ZoomAir Wireless Bridge default settings. Refer to the table on the next page:

Setting	**Default Value**
IP Address	192.168.0.240
IP Mask	255.255.255.0
Broadcast	192.168.0.255
SSID	Unique for each pair of Bridge units in a package
Channel	6
WEP State	Disabled
PassPhrase	User Determined
Beacon Period	80 time units
DTIM	2 beacon periods
Fragmentation Threshold	2304 octets
Authentication	Open System
RTS Threshold	2305 octets

Note: The following screen will be your starting point for navigation through ZoomAir Wireless Bridge Configuration mode dialog boxes:



Warning! As long as this session is active, modifications can be made to your Bridge's configuration. In order to exit this session it is neccesary to shut down your browser.

SSID and Channel Settings

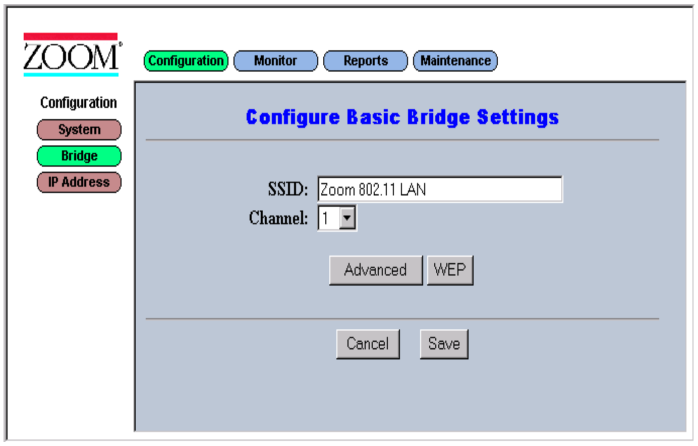
The SSID acts like a password; a snooper cannot link to your wireless bridge without knowing the SSID. Each pair of Bridge units is configured with a unique, randomly generated, shared SSID. Under most circumstances, there is no need to change this SSID. Note that if changed on one unit, it must be changed on the other as well.

The channel setting is the channel (equivalent to a cordless telephone channel) over which the Bridge units communicate.

You probably won't need to change the channel setting unless there is a nearby wireless device operating on the same or an adjacent channel.

Follow these steps to configure the SSID and channel settings:

1. On the **Configuration** page in WebManage, click **Bridge** on the left of the page. The **Configure Basic Bridge Settings** dialog box opens. See the following illustration:



Configure Basic Bridge Settings

SSID: Zoom 802.11 LAN
Channel: 1

2 The following are the details for configuring the wireless bridge settings:

SSID—The name of the wireless portion of your LAN. It is a unique string of characters that identifies the wireless Service Set ID of your LAN. The identifier also prevents outsiders from accessing your network if they do not know your SSID. ***Anyone using your network should regard the SSID as a password and keep it secret.***

Channel—Eleven channels are available for wireless LAN communication in North America; 13 are available in Europe. (Click on the down arrow to select a channel from the drop-down list.) These channels are much like the channels used by cordless telephones. Multiple cordless telephones can operate in close proximity, as long as each is set to a different channel. Similarly, many wireless data links can operate in the same area, as long as a clear channel is assigned to each link. The 802.11b standard utilizes bandwidth at about 2.4GHz. If there are competing uses for this spectrum near your ZoomAir Wireless Bridge, such as another wireless bridge, wireless LAN, or similar device, you may need to change the channel settings of your Bridge units from their default settings. You can assign up to three active channels among proximate links if they are at least five channels apart (e.g., 1, 6, 11).

Note 1: Wireless LANs installed in close proximity to your ZoomAir Wireless Bridge link may restrict the number of channels available to the Bridge because the Bridge shares bandwidth with wireless LANs.

Note 2: The functions of the **WEP** and **Advanced** buttons in the **Configure Basic Bridge Settings** dialog box (**page 23**) are explained in the WEP and Advanced Settings sections, respectively, later in this chapter.

3 Review the page when you have entered all the information. You can click **Cancel** if you want to restore the original values and start over. When you are satisfied with the information on this page, click **Save**. WebManage will send the information to the on-board memory in the ZoomAir Wireless Bridge, and you will see a confirmation message.

4 When you have successfully saved the new information, reboot the ZoomAir Wireless Bridge. To do that, on the main menu, click **Maintenance | Restart** to reboot. Set the current date and time whenever you restart the application. Bridge units do not have an internal clock.

Wired Equivalent Privacy (WEP)

As long as the SSID is kept secret, and if no other wireless 802.11b devices are within the range of your bridge, you probably do not need additional security measures. However, ZoomAir Wireless Bridge does provide for additional security in the form of Wired Equivalent Privacy. WEP addresses two security concerns:

- **Access Control**

  WEP allows you to provide an electronic “key” for your wireless bridge. It denies access to the bridge to anyone who does not have the key. Your Bridge units must exchange information about their current key before the bridge becomes active.

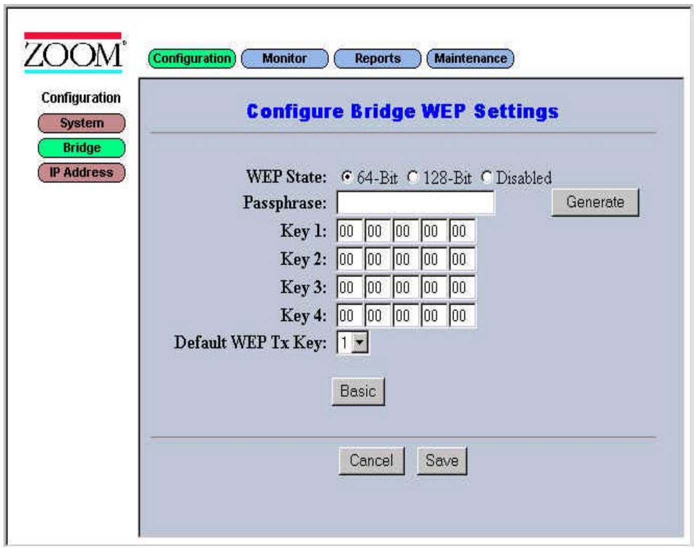
- **Eavesdropping Prevention**

WEP generates a pseudo-random number for each packet of information it sends. The packet contents cannot be decoded without knowledge of a shared secret key.

Note that bridge throughput will be reduced when WEP is activated.

Follow these steps to configure WEP settings:

1 On the **Configuration** page in WebManage, click **Bridge** on the left of the page. The **Configure Basic Bridge Settings** dialog box opens (see **page 23**). Then click the **WEP** button, and the **Configure Bridge WEP Settings** dialog box opens (see the next page):



Configure Bridge WEP Settings

WEP State: ● 64-Bit ○ 128-Bit ○ Disabled
Passphrase:
Key 1: 00 00 00 00 00
Key 2: 00 00 00 00 00
Key 3: 00 00 00 00 00
Key 4: 00 00 00 00 00
Default WEP Tx Key: 1

2 Click the **Security** button, and Choose one of the **WEP State** options:

- **64-Bit**—Enables 64-Bit WEP encryption. The peer Bridge unit also must have 64-Bit WEP enabled.
- **128-Bit**— Enables 128-Bit WEP encryption. The peer Bridge unit also must have 128-Bit WEP enabled.
- **Disabled**—Clients will not have access to WEP-

enabled clients and vice-versa. This option allows you to disable the WEP State security feature.

Note: Both Bridge units in a pair must have the same WEP state enabled (64-Bit, 128-Bit, or Disabled).

3. **Passphrase**—WEP generates its electronic keys (1-4) by converting the character string you enter in the **Passphrase** text box to a series of hexadecimal numbers. In the **Passphrase** text box, enter any string of characters.

   Click the **Generate** button to generate your WEP key. You can further modify the key by entering numbers directly into the keys 1-4.

   Default WEP Tx Key—This option allows you to create additional keys. You can create a set of four keys under each WEP Tx Key. The default setting is 1. Make sure you save any changes.

   Basic—Click this button to return to the **Configure Basic Bridge Settings** dialog box.

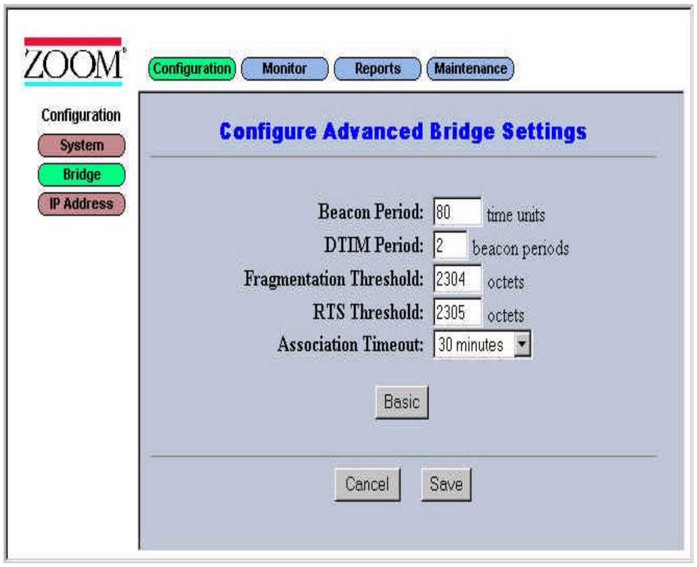
4. Review the page when you have entered all the information. You can click **Cancel** if you want to restore the original values and start over. When you are satisfied with the information on this page, click **Save**. WebManage will send the information to the on-board memory in the ZoomAir Wireless Bridge, and you will see a confirmation screen.

5. When you have successfully saved the new information, reboot the ZoomAir Wireless Bridge. To do that, on the main menu, click **Maintenance | Restart** to reboot.

Advanced Settings

The advanced settings for the wireless Bridge do not have an effect on access or security, and normally you do not need to change them. If you want to review them or if you have a reason to change them, follow these steps:

1. From the **Configure Basic Bridge Settings** page, click the **Advanced** button. The **Configure Advanced Bridge Settings** dialog box opens:



Configure Advanced Bridge Settings

Beacon Period: 80 time units
DTIM Period: 2 beacon periods
Fragmentation Threshold: 2304 octets
RTS Threshold: 2305 octets
Association Timeout: 30 minutes

2. The following are the details for filling in this dialog box:

Beacon Period—This sets the time between beacon transmissions of the ZoomAir Wireless Bridge. The default setting is 80 time units. The range is 20 to 32,767K time units. For a definition of "time unit", look up "Kusec" in the IEEE 802.11b specification.

DTIM Period—This value indicates the number of beacon periods between beacon transmissions that are Delivery Time Indicator Messages (DTIMs). Make any changes with care; this setting interacts with Beacon Period. The default is 2 beacon periods, with a range of 1 to 254.

Fragmentation Threshold—This parameter sets the point at which a long packet will be broken into fragments. The purpose of fragmentation is to increase the likelihood that long packets will get to their destination when there is high RF interference or where the radio unit is operating close to the limit of its range. Fragmentation reduces overall throughput. The default value is 2304 octets (an octet is 8 bits [1 Byte]). The range of possible entries is 256 to 2304 octets. The maximum value ensures that fragmentation is never used. Set the fragmentation threshold below the maximum only when you expect that the radio signal will sometimes be marginal.

RTS Threshold—The default setting is for the largest data packet allowed to pass between the ZoomAir Wireless Bridge units without activating the RTS/CTS flow control, which regulates the use of the radio spectrum. RTS/CTS is invoked automatically when data packets exceed the threshold value.

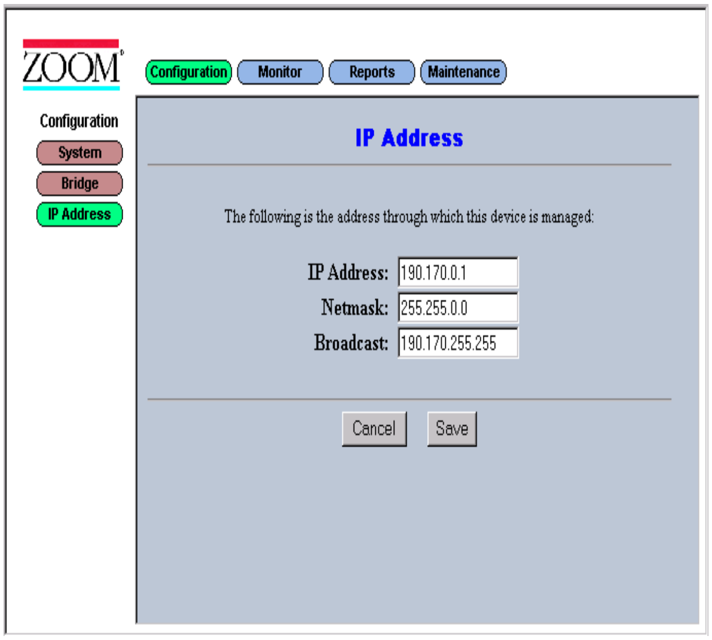
3 Review the dialog box settings when you have entered all the information. You can click **Cancel** if you want to restore the original values and start over. When you are satisfied with the information on this page, click **Save**. WebManage sends the information to the on-board memory in the ZoomAir Wireless Bridge, and you will see a confirmation message.

Note: You must then reboot the ZoomAir Wireless Bridge for your changes to take effect.

Device IP Address

To change the IP address of the ZoomAir Wireless Bridge unit, follow these steps:

1 Click on the **Configuration** button at the top of the page that you are on. Then click on the **IP Address** button on the left side of the page. The following screen displays (see the next page):



IP Address

The following is the address through which this device is managed:

IP Address: 190.170.0.1
Netmask: 255.255.0.0
Broadcast: 190.170.255.255

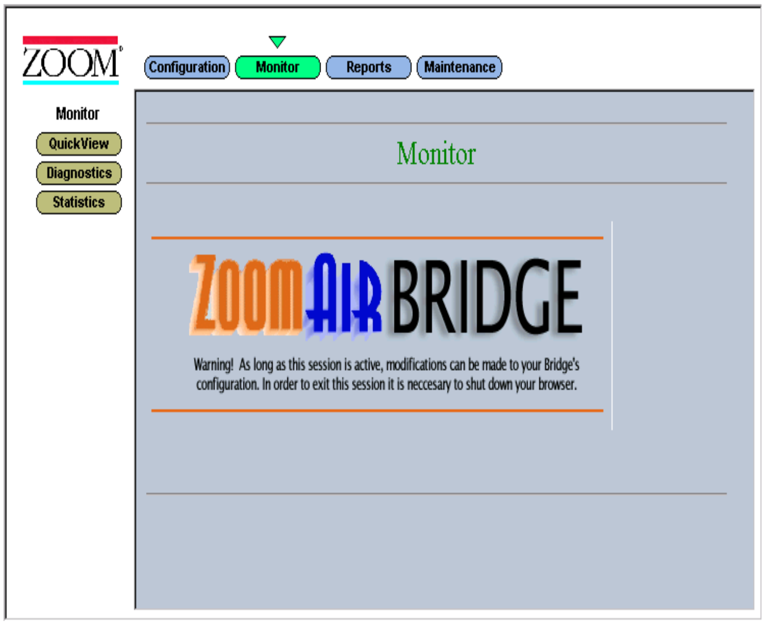
2 Fill in the **IP Address**, **Netmask**, and **Broadcast** boxes with the information you have obtained from your network system administrator. Click **Save**. To restore the original values and start over, click **Cancel**.

Note: The Netmask value is not generated automatically. Obtain it from your network system administrator.

3 When you have successfully saved the new information, reboot the ZoomAir Wireless Bridge. To do that, on the main menu, click **Maintenance | Restart** to reboot.

Monitoring the ZoomAir Wireless Bridge

The monitor screens in WebManage show you the state of the ZoomAir Wireless Bridge and its connections. Start your Internet browser and, in the **Address** box, type the IP address you have assigned to the Bridge unit you wish to monitor. Press **Enter**. The following page will appear:

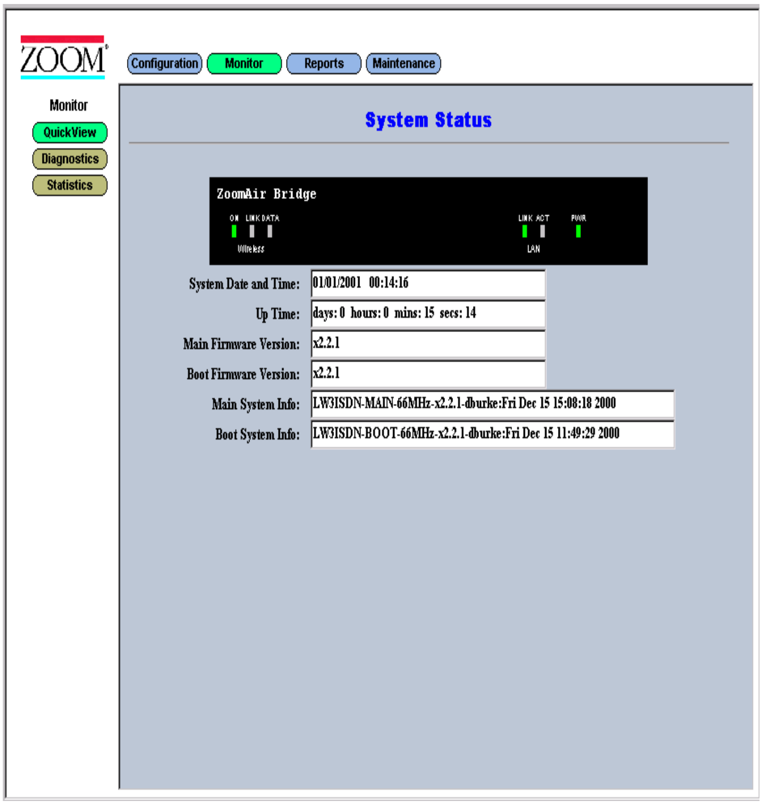


Warning! As long as this session is active, modifications can be made to your Bridge's configuration. In order to exit this session it is neccesary to shut down your browser.

Click the **Monitor** button on the top of the page. The buttons on the side of the page will change. The following sections briefly describe the function of each button.

QuickView Monitor

When you click on the **QuickView** button, you will see an image of the front panel of the ZoomAir Wireless Bridge unit, including its LED display (see the following screen shot). You will also see several entries depicting the amount of time the unit has been connected, the current firmware version, and other pertinent information.

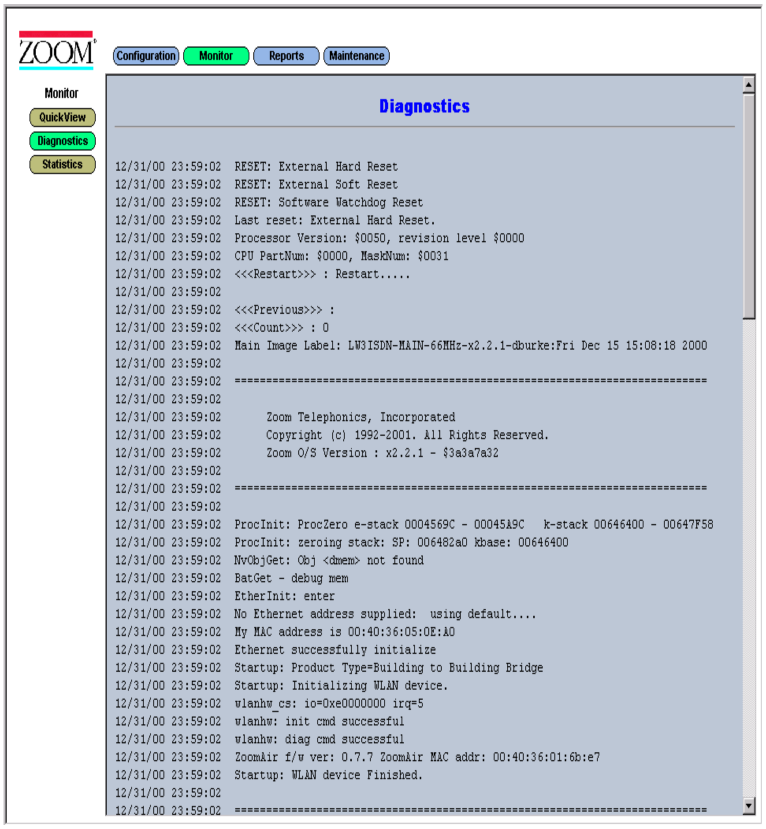


System Date and Time: 01/01/2001 00:14:16
Up Time: days: 0 hours: 0 mins: 15 secs: 14
Main Firmware Version: x2.2.1
Boot Firmware Version: x2.2.1
Main System Info: LW3ISDN-MAIN-66MHz-x2.2.1-dburke:Fri Dec 15 15:08:18 2000
Boot System Info: LW3ISDN-BOOT-66MHz-x2.2.1-dburke:Fri Dec 15 11:49:29 2000

Note: Information on the COL LED is not available on this screen.

Diagnostics Monitor

In Monitor mode, click on the **Diagnostics** button to see the **Diagnostics** page. This page shows detailed information about the functioning of the ZoomAir Wireless Bridge. It is useful as a troubleshooting tool. If you need to contact your vendor or Zoom Technical Support for help, you should include the log from the **Diagnostics** page in your e-mail message or fax. The following is an illustration of the Diagnostics Monitor:



Diagnostics

```
12/31/00 23:59:02  RESET: External Hard Reset
12/31/00 23:59:02  RESET: External Soft Reset
12/31/00 23:59:02  RESET: Software Watchdog Reset
12/31/00 23:59:02  Last reset: External Hard Reset.
12/31/00 23:59:02  Processor Version: $0050, revision level $0000
12/31/00 23:59:02  CPU PartNum: $0000, MaskNum: $0031
12/31/00 23:59:02  <<<Restart>>> : Restart.....
12/31/00 23:59:02
12/31/00 23:59:02  <<<Previous>>> :
12/31/00 23:59:02  <<<Count>>> : 0
12/31/00 23:59:02  Main Image Label: LW3ISDN-MAIN-66MHz-x2.2.1-dburke:Fri Dec 15 15:08:18 2000
12/31/00 23:59:02
12/31/00 23:59:02  ============================================================================
12/31/00 23:59:02
12/31/00 23:59:02       Zoom Telephonics, Incorporated
12/31/00 23:59:02       Copyright (c) 1992-2001. All Rights Reserved.
12/31/00 23:59:02       Zoom O/S Version : x2.2.1 - $3a3a7a32
12/31/00 23:59:02
12/31/00 23:59:02  ============================================================================
12/31/00 23:59:02
12/31/00 23:59:02  ProcInit: ProcZero e-stack 0004569C - 00045A9C   k-stack 00646400 - 00647F58
12/31/00 23:59:02  ProcInit: zeroing stack: SP: 006482a0 kbase: 00646400
12/31/00 23:59:02  NvObjGet: Obj <dmem> not found
12/31/00 23:59:02  BatGet - debug mem
12/31/00 23:59:02  EtherInit: enter
12/31/00 23:59:02  No Ethernet address supplied:  using default....
12/31/00 23:59:02  My MAC address is 00:40:36:05:0E:A0
12/31/00 23:59:02  Ethernet successfully initialize
12/31/00 23:59:02  Startup: Product Type=Building to Building Bridge
12/31/00 23:59:02  Startup: Initializing WLAN device.
12/31/00 23:59:02  wlanhw_cs: io=0xe0000000 irq=5
12/31/00 23:59:02  wlanhw: init cmd successful
12/31/00 23:59:02  wlanhw: diag cmd successful
12/31/00 23:59:02  ZoomAir f/w ver: 0.7.7 ZoomAir MAC addr: 00:40:36:01:6b:e7
12/31/00 23:59:02  Startup: WLAN device Finished.
12/31/00 23:59:02
12/31/00 23:59:02  ============================================================================
```

Statistics Monitor

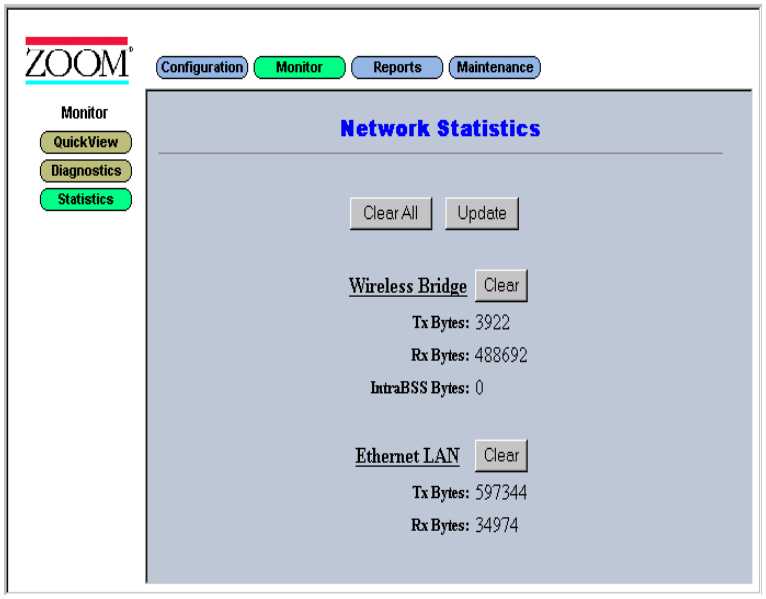
In Monitor mode, click on the **Statistics** button to see the **Network Statistics** page. On this page (see the next screen shot), you can monitor the data transfer between:

- Two ZoomAir Wireless Bridge units, under **Wireless Bridge**
- A PC and a ZoomAir Wireless Bridge unit on a wired network, under **Ethernet LAN**.

Click **Clear All** to reset to zero all the displayed data transfer readings.

Click **Update** to see the most recent data transfer readings. The statistics are updated every few seconds.

Click **Clear** to reset to zero the values shown under either **Wireless Bridge** or **Ethernet LAN**.



Network Statistics

Wireless Bridge

Tx Bytes: 3922

Rx Bytes: 488692

IntraBSS Bytes: 0

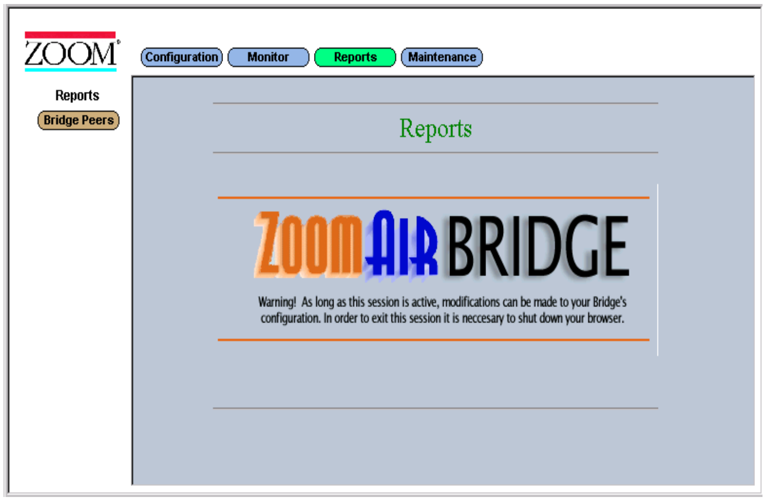
Ethernet LAN

Tx Bytes: 597344

Rx Bytes: 34974

Using the ZoomAir Wireless Bridge Reports

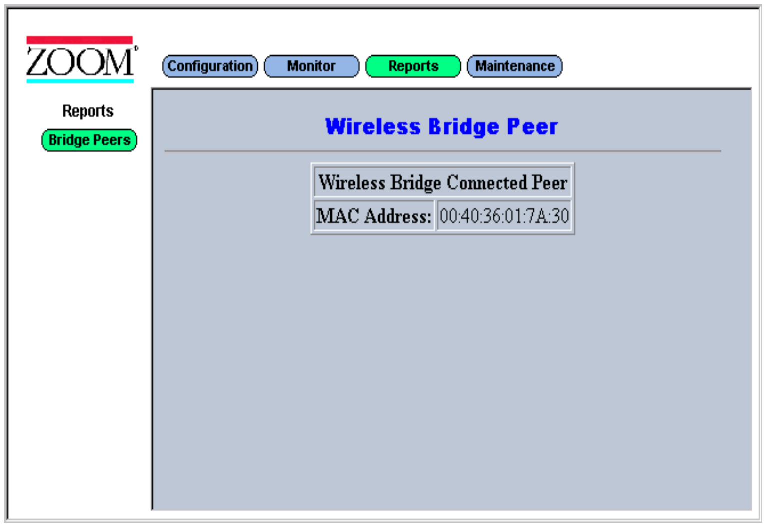
This feature allows you to verify and identify the peer connection. The following screen will be your starting point for navigation through ZoomAir Wireless Bridge Reports mode dialog boxes:



Reports

Warning! As long as this session is active, modifications can be made to your Bridge's configuration. In order to exit this session it is neccesary to shut down your browser.

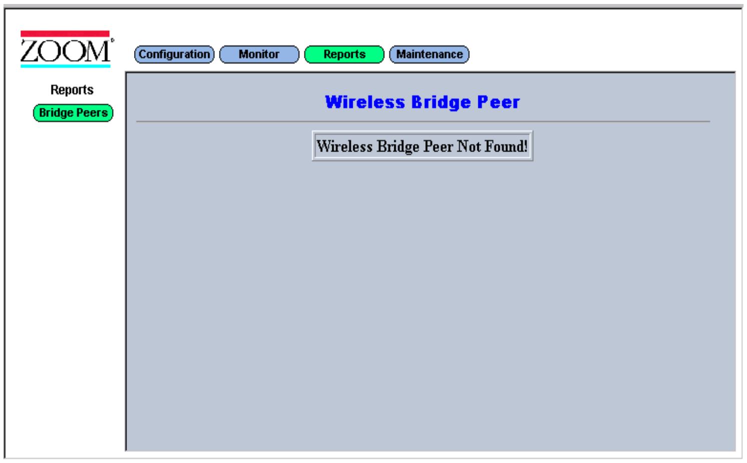
Click the **Reports** button on the top of the **Reports** page, and then click **Bridge Peers** on the side of the page. The **Wireless Bridge Peer** screen displays:



Wireless Bridge Peer

Wireless Bridge Connected Peer	
MAC Address:	00:40:36:01:7A:30

Shown in the table is the MAC Address (a device-associated unique identifier) of the ZoomAir Card in the peer Bridge unit. If that ZoomAir Card is not detected, the following screen displays:



Wireless Bridge Peer

Wireless Bridge Peer Not Found!

If the ZoomAir Card in the peer Bridge unit was not detected, no wireless link between the Bridge units was established. If this is the case, make sure there are no interfering installations nearby. RF (radio frequency) devices can interfere with your wireless link. Among such devices are cordless phones, video surveillance systems, digital handsets, walkie-talkies, Home RF devices, and devices that are part of other 802.11 wireless networks.

If there is still no link, experiment with the antenna cables. For example, if you are in your trial setup, disconnect the cables and antennas on both sides of your wireless bridge, and repeat the antenna installation and orientation carefully. Make sure the antennas are facing each other, as explained on **page 14**.

If you are still unable to detect the peer ZoomAir Card from either of your Bridge units, it is likely that the configuration of the Bridge is not proper.

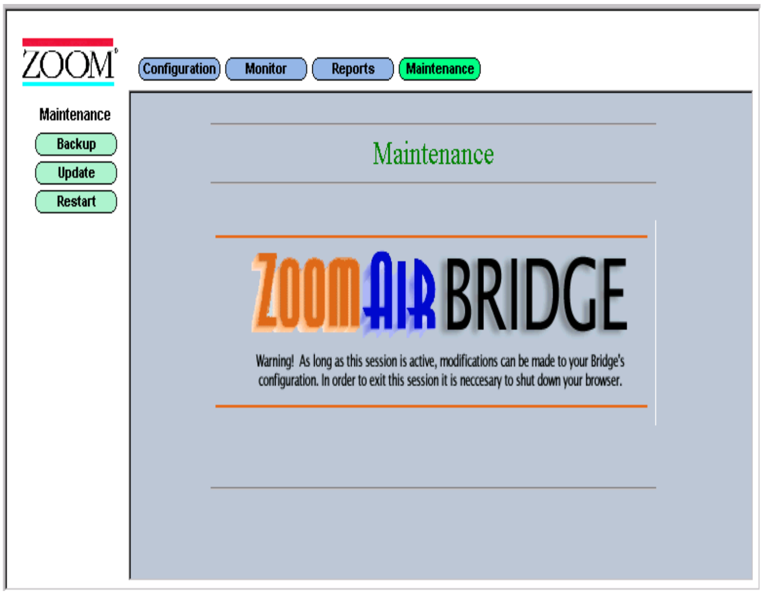
Maintaining the ZoomAir Wireless Bridge

Maintaining the firmware on the ZoomAir Wireless Bridge board is simple and consists of the following procedures:

- Accessing Maintenance in WebManage
- Updating the firmware with Backup System code
- Restarting the ZoomAir Wireless Bridge unit.

Accessing Maintenance in WebManage

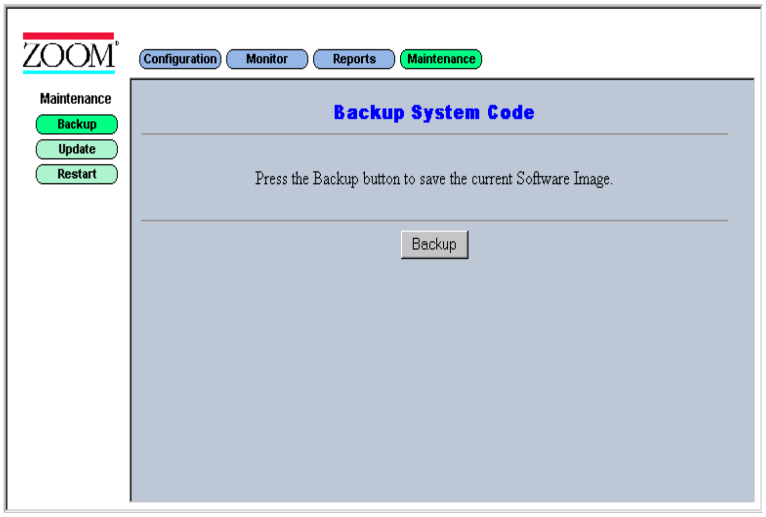
Start your Internet browser and, in the address box, type in the IP address you have assigned to it. Press **Enter**. Click on the **Maintenance** button on the top of the **Maintenance** splash screen, shown next. The following sections describe the functions of the buttons on the side of the **Maintenance** page.



Warning! As long as this session is active, modifications can be made to your Bridge's configuration. In order to exit this session it is neccesary to shut down your browser.

Backup System Code

The Backup feature helps you save the image of your current software. We recommend that you save the current software image before updating the system software. To back up the current software image, click on the **Backup** button on the left side of the page. The following screen appears:



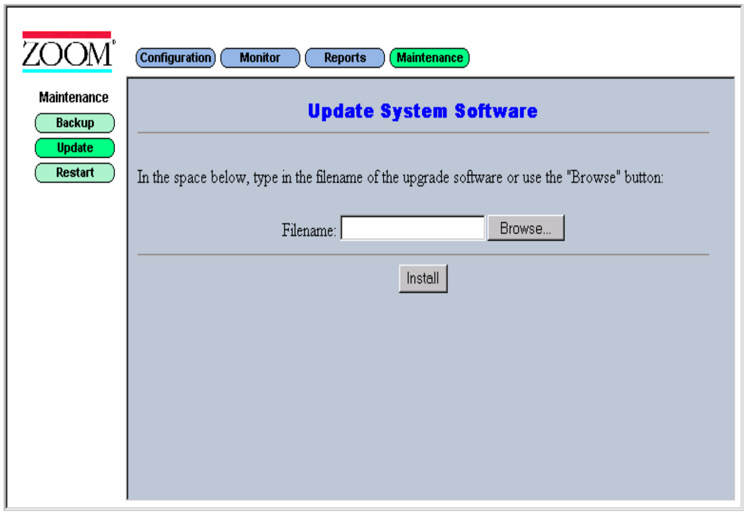
Backup System Code

Press the Backup button to save the current Software Image.

Click the **Backup** button in the middle of the page to save the current software image to a drive. (The **C** drive is the default. You can also save the image on a floppy disk.) This function allows you to retain a copy of the original software image when upgrading new software. You can reload the original image at any time.

Upgrading the System Software

Clicking on **Update** will take you to the following screen:



Update System Software

In the space below, type in the filename of the upgrade software or use the "Browse" button:

Filename:

Here you need to specify the name of the file. You can either type in the name of the file or click on **Browse** and choose it from the list. Click **Install** after selecting the correct file.

The **File Update Report** page will appear. If you have entered the correct filename, you will see the message

```
System Upload SUCCESSFUL
```

If you have selected the wrong filename (or typed it incorrectly), you will see the message

```
System Upload FAIL
```

Check that you are using the right filename and directory name and repeat the procedure.

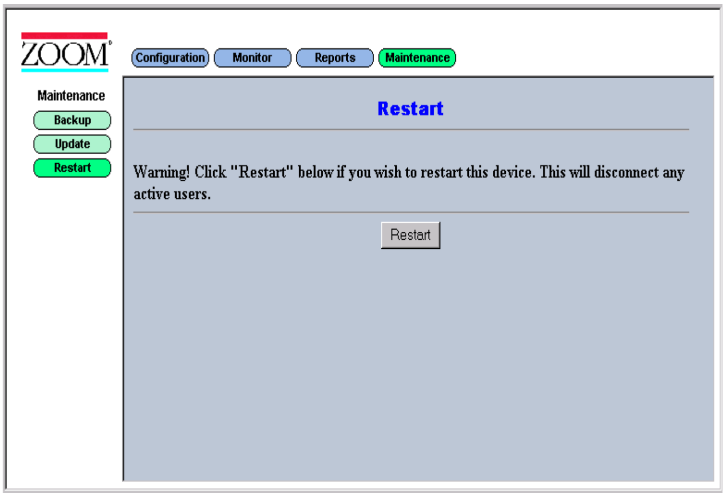
When the upload is successful, you will see the following message:

```
Please restart ZoomAir Bridge…
```

Click **Restart**.

Restarting the ZoomAir Wireless Bridge

In Maintenance mode, click on the **Restart** button on the left side of the screen in order for your updates to be accepted and take effect. The following screen appears:



Warning! Click "Restart" below if you wish to restart this device. This will disconnect any active users.

Click **Restart** in the middle of the page. You must do this in order for the changes you have made to take effect. Exit your browser.

Appendix A

Assigning New IP Addresses to ZoomAir Wireless Bridge Units

The two ZoomAir Wireless Bridge units in your package initially have the same factory default IP address. To manage the Bridge units, however, each must have a unique IP address, provided by your systems network administrator. You can use the console to assign a unique IP address to each of your Bridge units.

First, make sure that you do the following:

- Plug the power adapter into the 12-VDC jack at the back of the ZoomAir Wireless Bridge unit. Then plug the power cable into an AC outlet.
- Turn on the power switch at the back of the ZoomAir Wireless Bridge unit.
- Plug the RJ-45 connector of the included serial cable (RS-232) into the console port on the ZoomAir Wireless Bridge.
- Plug the other end of the serial cable into the DB-9 connector.
- Plug the DB-9 connector (female) into the serial (COM) port (male) of the control console PC that will run a terminal program (e.g., HyperTerminal).

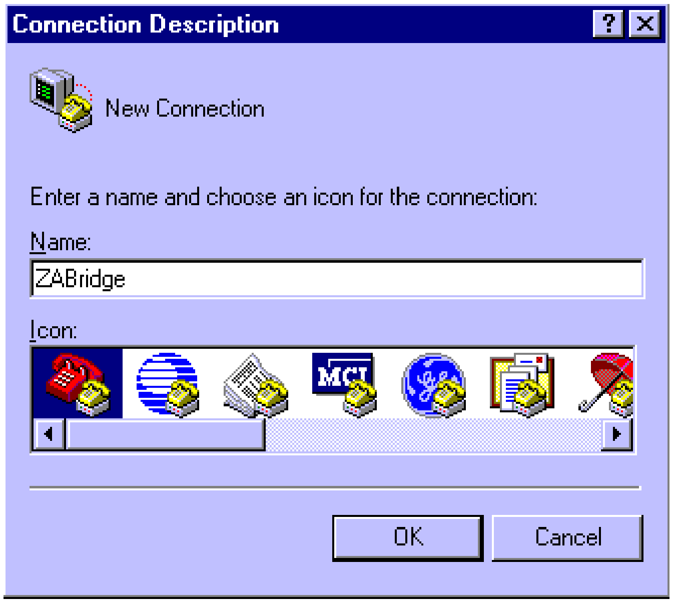
Note: You may also need a second adapter to match the DB-9 adapter to your computer's serial port: a DB-9 to DB-25 adapter for a PC or a DB-9 to 8-pin Mini-DIN for a Macintosh. See your computer documentation for more details.

Then, follow these steps:

1 Open the HyperTerminal on the PC that is connected to the ZoomAir Wireless Bridge unit:

Click **Start** | **Programs** | **Accessories** | **HyperTerminal**.

Double-click **hypertrm.exe**. The **Connection Description** dialog box opens:

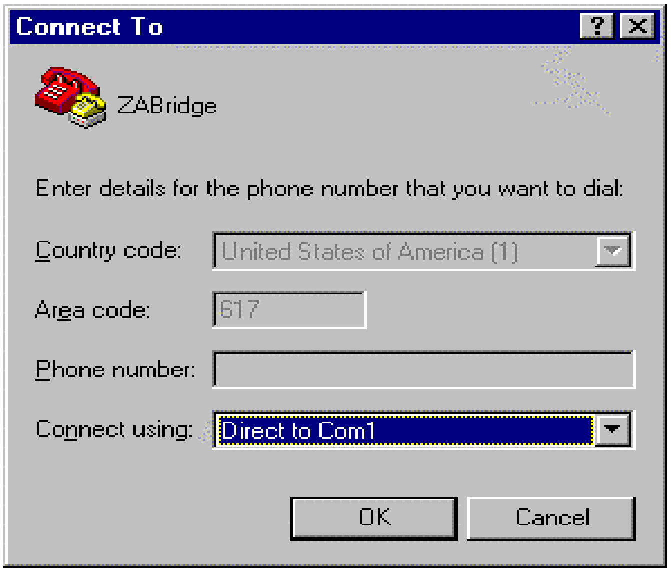


Enter a name and choose an icon for the connection:

Name: ZABridge

Type in a name for the connection and click **OK**.

2 The **Connect To** dialog box opens:



Enter details for the phone number that you want to dial:

Country code: United States of America (1)

Area code: 617

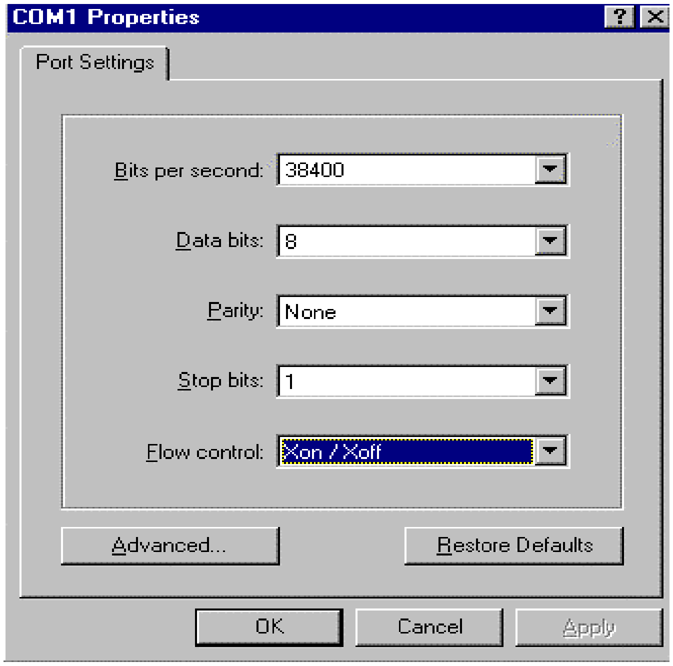
Phone number:

Connect using: Direct to Com1

In the window, next to **Connect using**, select the port on your PC to which the console cable is connected. The usual setup is **Direct to Com1** or **Direct to Com2**, depending on which port the RS-232 cable is connected to (COM1 or COM2).

Click **OK**.

3 The **Port Settings** tabbed page appears:



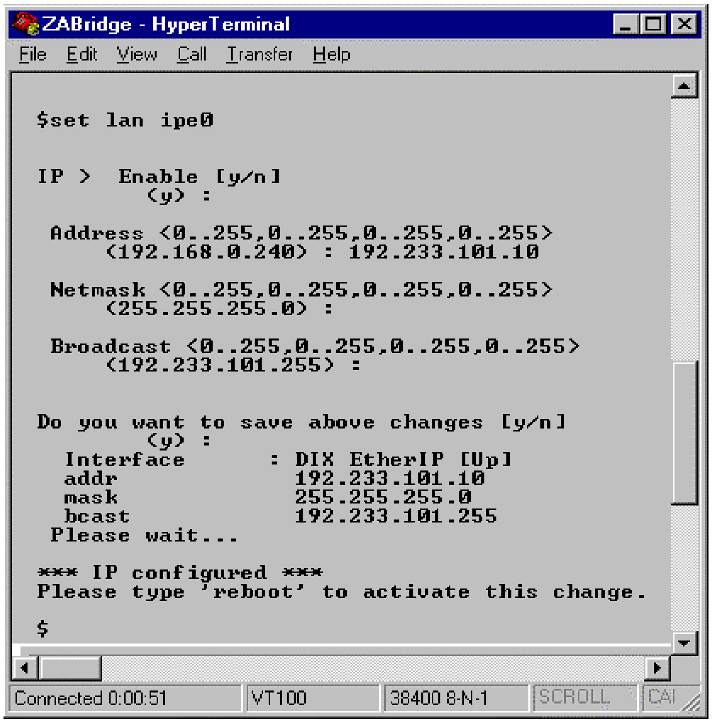
Bits per second: 38400
Data bits: 8
Parity: None
Stop bits: 1
Flow control: Xon / Xoff

4 In **Port Settings**, select the settings in the text boxes as follows:

- **Bits per second:** 38400
- **Data bits:** 8
- **Parity:** None
- **Stop bits:** 1
- **Flow control:** Xon/Xoff

Click **OK**.

5 The **HyperTerminal** text box opens:



```
$set lan ipe0


IP >  Enable [y/n]
        (y) :

 Address <0..255,0..255,0..255,0..255>
     (192.168.0.240) : 192.233.101.10

 Netmask <0..255,0..255,0..255,0..255>
     (255.255.255.0) :

 Broadcast <0..255,0..255,0..255,0..255>
     (192.233.101.255) :


Do you want to save above changes [y/n]
        (y) :
  Interface      : DIX EtherIP [Up]
  addr             192.233.101.10
  mask             255.255.255.0
  bcast            192.233.101.255
 Please wait...

*** IP configured ***
Please type 'reboot' to activate this change.

$
```

6 Press **Enter**. At the **$** prompt, type `set lan ipe0`. **Enter**.

7 At **IP > Enable (y/n)**, press **Enter** to select **y**.

8 Enter the new IP address when prompted, and press **Enter**. The default Netmask value appears. You can accept it or change it. Press **Enter**.

9 Accept the default Broadcast value by pressing **Enter**.

10 When asked **Do you want to accept above changes (y/n)**, press **Enter** to select **y**.

11 Type **reboot** to activate the changes.

Ping Testing the ZoomAir Wireless Bridge-PC Connection

You can perform the ping test to isolate problems with your wireless bridge and network (PING—Packet Internet Groper). “Pings” are special packets that are sent to a particular device (with a specific IP address). This device reflects (or pings) the packet back to the sender. In this way, both the send and receive paths are verified. By carefully choosing ping endpoints, you can determine whether a problem with your bridge resides in the wireless link or in the connection of one or more of the Bridge units to their respective LAN segments.

Note: Before ping testing, make sure TCP/IP is installed.

When you perform the ping test, if response times are displayed, the ping has been successful. If a ping times out, the ping has failed.

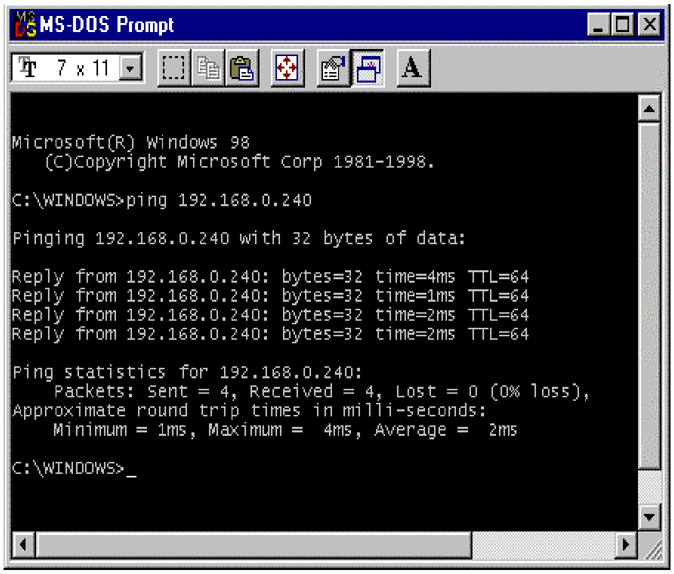
To isolate a problem in the network and/or wireless bridge, ping-test each connection that you have made. First, ping-test a Bridge unit from the console of the peer Bridge unit. Ping from one Bridge unit to the other, sending ping from the console of one unit. To do this, from the console of a Bridge unit, type

```
%ping <IP address>
```

where “IP address” is the IP address that you assigned to the peer Bridge unit. If this ping fails, the wireless link isn’t working. If you succeed with this test, then the fault is elsewhere.

Next, ping from a PC to the local Bridge unit. To do this, make sure the PC is connected to the Bridge unit (as described earlier in this chapter and in Appendix A) and type `ping` followed by the IP address that you assigned to the peer Bridge unit. Follow these steps:

1. On a PC connected to the bridged network, click **Start | Programs**.
2. Click on **MS-DOS Prompt**. The **MS-DOS Prompt** dialog box opens:



```
Microsoft(R) Windows 98
   (C)Copyright Microsoft Corp 1981-1998.

C:\WINDOWS>ping 192.168.0.240

Pinging 192.168.0.240 with 32 bytes of data:

Reply from 192.168.0.240: bytes=32 time=4ms TTL=64
Reply from 192.168.0.240: bytes=32 time=1ms TTL=64
Reply from 192.168.0.240: bytes=32 time=2ms TTL=64
Reply from 192.168.0.240: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.0.240:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum =  4ms, Average =  2ms

C:\WINDOWS>_
```

3. At the **C:\WINDOWS>** prompt, type `ping`, followed by the IP address of the Bridge unit.

   If the PC and the Bridge unit are connected, you will receive a reply from the Bridge unit. If there is no connection, you will receive the **Request timed out** system response.

Also make sure that:

- The ZoomAir Wireless Bridge units are receiving power.
- The ZoomAir Cards are firmly plugged in. A slowly flashing green light on the ZoomAir Card indicates that the card is linked to the network.

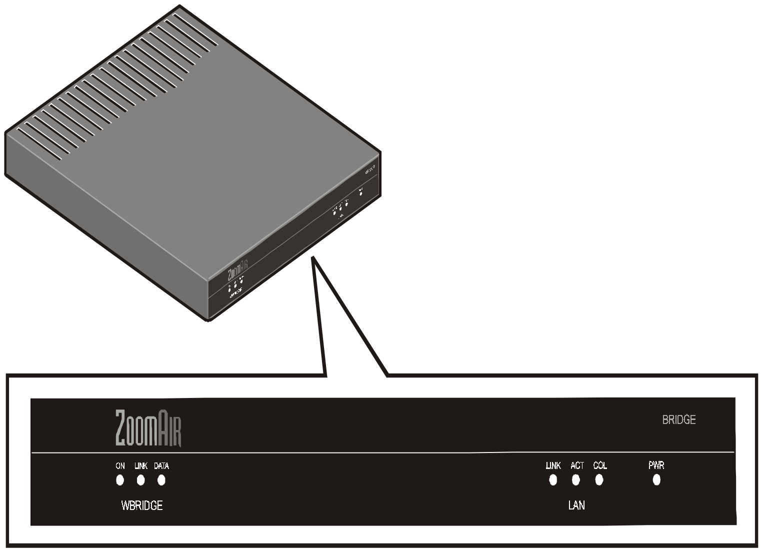
  Remember: the ZoomAir Cards cannot be hot-swapped. You must power down each time you remove a ZoomAir Card.
- The two ZoomAir Wireless Bridge units are set to the same SSID, the same channel, and have the same WEP key, if one is used.
- The antennas are oriented correctly.

If the bridge ping succeeds, test the link from a network PC to the local ZoomAir Wireless Bridge unit. Repeat for the opposite side of the bridge link.

Appendix B

LED Indicators

The front panel of the ZoomAir Wireless Bridge contains seven LEDs that will help you monitor and troubleshoot your LAN and wireless connection.



LAN LED Indicators

The four LEDs relating to the ZoomAir Wireless Bridge LAN settings are **LINK, ACT, COL,** and **PWR**.

LINK — This green LED shows that the 10BaseT Ethernet port link is working correctly.

ACT — Short for Activity, this green LED indicates that the 10BaseT Ethernet port is transmitting or receiving packets.

COL — Short for Collision, this red LED indicates that the network is experiencing traffic collisions. No action is necessary.

PWR — This green LED on the far right of the panel lights up and remains on when you push the on/off switch on the back panel of the ZoomAir Wireless Bridge.

Wireless LED Indicators

The three green LEDs **— ON**, **LINK**, and **DATA—** located under the ZoomAir logo, pertain to your wireless bridge:

ON — The radio card is receiving power.

LINK — The unit has located its peer.

DATA — The unit is receiving and/or transmitting data.

Appendix C

Console Commands

You may prefer to program the ZoomAir Wireless Bridge from the console rather than from the browser-based WebManage. If your WebManage connection is terminated (for whatever reason), you can use the console to restart the Bridge and WebManage.

Setting Up the Console

Once you've connected the ZoomAir Wireless Bridge to your computer using the supplied console cable, follow these steps:

1. Start any terminal application that can be set to a serial rate of exactly 38.4 Kbps. The HyperTerminal application that comes with Windows 95/98 and NT is a good example. To illustrate, click on **Start | Programs |Accessories | HyperTerminal**. The **Connection Description** box will pop up. Type in the name of your new connection (a name of your choice) and double-click on an icon to represent it. Hit **Enter**.
2. You will be asked how you want to connect. Ignore the phone number entry. Under **Connect using**, select the same COM port as that used to connect the console to the ZoomAir Wireless Bridge. Click **OK**. The **COM Properties** dialog box will open. Under **Bits per second**, select **38400**. **Data bits** will be set to **8**; **Parity** will be set to **none**; **Stop bits** will be set to **1**; leave all three as-is. Under **Flow control**, select **Xon/Xoff**. Click **OK**. Hit **Enter** to get a **$** in the terminal window.

Note: If your connection attempt fails, double-check that your serial cable connection is secure and that your COM port selections match.

Configuring Other Parameters

Get Commands: Viewing the Configuration

The tables on the following pages categorize the **get** commands and their functions.

get commands

If you type **get** followed by…	the console will display…
system	The system parameters
lan	The TCP/IP address information
bridge	The details of your Bridge configuration, such as security
version	The build version of the Bridge software
sysinfo	The detailed system parameters, which will be helpful if you need to call Tech Support
mac	The MAC (Media Access Control address) of the Bridge
ntp	The Network Time Protocol – the time assigned from the network to the Bridge unit

get system commands

If you type **get system** followed by…	The console will display…
username	The username of the Bridge unit
date	The current system date
time	The current system date and time
timezone	The time zone of the Bridge system
devname	The name of the Bridge unit and the first part of its MAC address
contact	The system administrator’s name
location	The location of the Bridge unit

get lan command

If you type **get lan** followed by…	The console will display…
ipe0	The Bridge TCP/IP address and other pertinent information such as mask and broadcast addresses

get bridge commands

If you type **get bridge** followed by…	the console will display…
basic	The Bridge configuration parameters such as channel and SSID (special identifier I.D.)
advanced	Additional Bridge parameters such as fragmentation threshold and beacon period

security	The security parameters such as WEP (Wired Equivalency Protocol) settings and the Passphrase
status	The current Bridge peer unit association

Set Commands: Changing the Configuration

The following tables categorize the **set** commands and their functions.

set commands

If you type **set** followed by…	the console will display…
system	The system parameters
lan	The TCP/IP address information
bridge	The details of your Bridge configuration
ntp	The details of network time protocols

set system commands

If you type **set system** followed by…	the console will display…
username	The username of the Bridge unit
devname	The name of the Bridge unit and the first part of its MAC address
contact	The system administrator's name
location	The location of the Bridge unit
password	The password of the Bridge system administrator
date	The current system date

time	The current system time
timezone	The time zone for which the time is shown

set lan commands

If you type **set lan** followed by…	the console will display…
ipe0	The Bridge TCP/IP address and other pertinent information such as mask and filter profile

set bridge commands

If you type **set bridge** followed by…	the console will display…
basic	The default Bridge parameters
advanced	The more detailed Bridge configuration parameters
security	The security parameters such as WEP settings

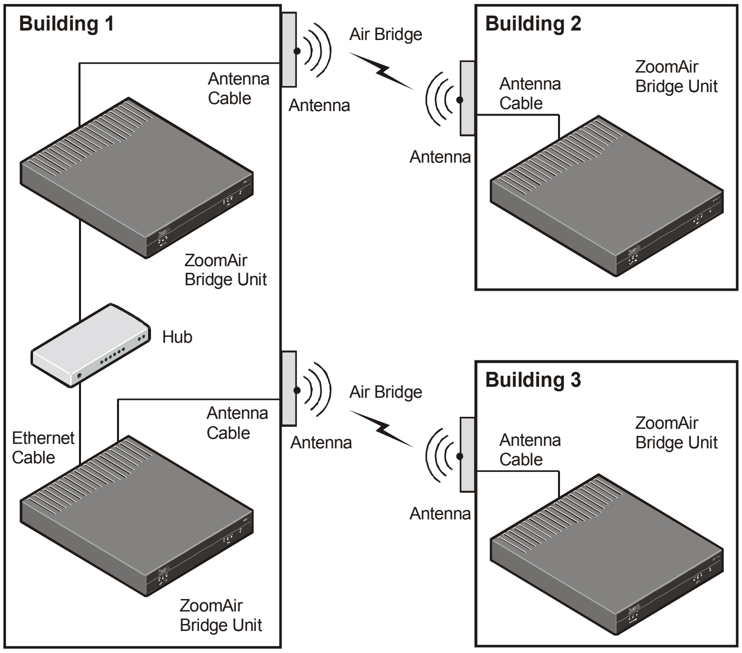
Appendix D

Three-Way Wireless Bridge Setup

You can create a wireless bridge to connect wired LANs in three different buildings. To do this, create two distinct bridge links, where a central building hosts two Bridge units that link the other two buildings. The following are the required settings for these two Bridge pairs:

- They must have different SSIDs
- They must use different channels, with a channel difference of five.

The following is an illustration of a three-way bridge setup:



Appendix E

Regulatory Information

ZoomAir Wireless Bridge

FCC Part 15 Emissions Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Part 68 Statement

This equipment complies with Part 68 of the FCC rules. The unit bears a label which contains the FCC registration number and Ringer Equivalence Number (REN). If requested, this information must be provided to the telephone company.

This equipment uses the following standard jack types for network connection: RJ11C.

This equipment contains an FCC-compliant modular jack. It is designed to be connected to the telephone network or premises wiring using compatible modular plugs and cabling which comply with the requirements of FCC Part 68 rules.

The Ringer Equivalence Number, or REN, is used to determine the number of devices that may be connected to the telephone line. An excessive REN may cause the equipment to not ring in response to an incoming call. In most areas, the sum of the RENs of all equipment on a line should not exceed five (5.0).

In the unlikely event that this equipment causes harm to the telephone network, the telephone company can temporarily disconnect your service. The telephone company will try to warn you in advance of any such disconnection, but if advance notice isn't practical, it may disconnect the service first and notify you as soon as possible afterwards. In the event such a disconnection is deemed necessary, you will be advised of your right to file a complaint with the FCC.

From time to time, the telephone company may make changes in its facilities, equipment, or operations that could affect the operation of this equipment. If this occurs, the telephone company is required to provide you with advance notice so you can make the modifications necessary to obtain uninterrupted service.

U.S. REPAIR CENTER INFORMATION:

Zoom Telephonics, Inc.
645 Summer Street
Boston, MA 02210
USA
Telephone Number: (617) 423 1072
Facsimile Number: (617) 542 8276

There are no user serviceable components within this equipment.

It shall be unlawful for any person within the United States to use a computer or other electronic device to send any message via a telephone facsimile unless such message clearly contains, in a margin at the top or bottom of each transmitted page or on the first page of the transmission, the date and time it is sent and an identification of the business, other entity, or individual sending the message and the telephone number of the sending machine or of such business, other entity, or individual. The telephone number provided may not be a 900 number or any other number for which charges exceed local or long distance transmission charges. Telephone facsimile machines manufactured on and after December 20, 1992, must clearly mark such identifying information on each transmitted message. Facsimile modem boards manufactured on and after December 13, 1995, must comply with the requirements of this section.

This equipment cannot be used on public coin phone service provided by the telephone company. Connection to Party Line Service is subject to state tariffs. Contact your state public utility commission, public service commission, or corporation commission for more information.

Declaration of Conformity

The manufacturer declares under sole responsibility that this equipment is compliant to Directive 1999/5/EC (R&TTE Directive) via the following standards:

Standards

EN 60950: 1992 incorporating amendments 1 to 4
EN 55024: 1998
EN 55022: 1998
The product is CE Marked.

11MB ZoomAir Card

FCC Part 15 Emissions Statement

All wireless LAN devices generate radio frequency energy and if not installed and used properly, i.e., in strict accordance with these instructions, may cause interference to radio and television reception. This device has been tested and found to comply with the limits for a Class B Computing Device in accordance with the specification in Subpart B of Part 15 of the FCC Rules, which are designed to provide reasonable protection against such interference in a residential installation.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause interference to radio and television reception, which can be determined by turning the equipment off and on, try to correct the interference by one or more of the following measures:

- Relocate the receiving antenna.
- Relocate the device with respect to the receiver.
- Move the device away from the receiver.
- Plug the device into a different outlet so that the device and receiver are on different branch circuits.
- If necessary, consult the dealer or an experienced radio/television technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

FCC Warning

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Caution: For the purpose of satisfying FCC RF exposure compliance requirements, antennas should be positioned in such a way that a separation distance of at least 20cm is maintained between the transmitter's radiating structures and the body of the user or nearby persons.

FCC Part 15 C Statement

This equipment is approved under Subpart C of FCC Part 15, under the FCC Identifier BDNWLNPCCARD11.

Department of Commerce End User Statement

This item falls under the jurisdiction of the Department of Commerce, and as such, the requirement set forth in section 740-17 of the Export Administration Regulation must be complied with. See the following Web sites for more information:

- ☐ Bureau of Export Administration

  http://www.bxa.doc.gov/DPL/2_denial.htm

  http://www.bxa.doc.gov/Entities/

- ☐ Code of Federal Regulations

  http://www.access.gpo.gov/bxa/car/ear_data.html

Federal law prohibits the sale or distribution of certain products to certain individuals and organizations. Denied persons or organizations may not, directly or indirectly, participate in any way in any transaction involving any commodity, software or technology exported or to be exported from the United States that is subject to Export Administration Regulations. The above Web sites provide a detailed list of individuals and organizations that have been determined to present an unacceptable risk of diversion to developing weapons of mass destruction or missiles used to deliver those weapons.

Declaration of Conformity

The manufacturer declares under sole responsibility that this equipment complies with Directive 1990/5/EC (R&TTE Directive) via the following standards:

Standards

EN 60950 : 1992 incorporating Amendments 1 to 4

EN 55022 : 1998

EN 61000-4-3 : 1994

EN 61000-4-2 : 1995

ETS 300 328 : 1996

ETS 300 826 : 1997

The product is CE marked.

Intended Use

The intended use for this RLAN equipment is operation in the 2.4GHz frequency band.

©2001